# 安全-RSA（BUUCTF）

原创

小狐狸FM 于 2021-08-09 17:19:16 发布 170 收藏

分类专栏： 安全 # CTF夺旗 文章标签： python rsa



本文链接：https://blog.csdn.net/smallfox233/article/details/119542322



安全 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏


CTF夺旗

38 篇文章 0 订阅

订阅专栏

## 文章目录



## 前言

> 如果安装 `gmpy2` 的时候报错，可以看下方的文章

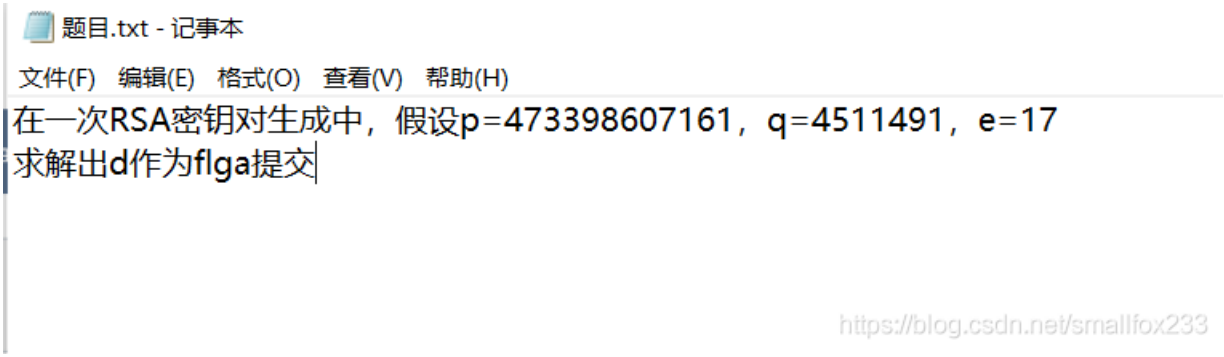
Python-解决下载gmpy2的报错问题

安全-RSA算法基础

## 一、题目

题目链接







## 二、WriteUp

> RSA的公式如下:

$n = p*q$

$\varphi(n) = (p-1)*(q-1)$

$c = ( m^e ) \bmod n$

$d = 1 \bmod \varphi(n) / e$

$m = ( c^d ) \bmod n$

- 其中已知的三个量是 `e` 、 `p` 和 `q` ，所以可以先计算欧拉函数再计算 `d` 的值
- 先算出欧拉函数 `ϕ(n)` 的值，然后调用 `gmpy2` 的库实现 `1 mod ϕ(n) / e`

```
p:473398607161
q:4511491
e:17
125631357777427553
>>>
```



```python
# coding=utf-8
# 作者：小狐狸FM
import gmpy2
p = int(input("p:"))
q = int(input("q:"))
e = int(input("e:"))
fn = (p-1) * (q-1) #计算欧拉函数
print(gmpy2.invert(e, fn))
```